UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/708,263	11/07/2000	Kiyoshi Ogishi		9975

7590 03/16/2005

Hogan & Hartson L.L.P
500 South Grand Avenue, Suite 1900
Los Angeles, CA 90071

EXAMINER	
ADAMS, JONATHAN R	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/708,263	OGISHI ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 4, 8, and 10 have been amended

Claims 21-23 have been added

Response to Arguments

2. Applicant's arguments filed 10/19/04 have been fully considered but they are not persuasive.

3. In regard to applicant's argument that the references do not teach generating a secret key of each entity by using a mapping at a point on an algebraic curve, the examiner disagrees. Tanaka teaches generation (Col 1, Fig 3 and 4, Tanaka) of a secret keys [gl1, gl2] of each entity by using a mapping at a point on an algebraic curve (Col 1, Fig 3 and 4, Tanaka).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1, 2, 4, and 12-23 rejected under 35 U.S.C. 102(b) as being preceded by Hatsukazu Tanaka, "Security Certified Identity-based Non-Interactive Key Sharing" (hereafter referred to as Tanaka).

2. As to claim 1, Tanaka discloses an identity based cryptosystem comprising:

- Generating a secret key by mapping at a point on an algebraic curve / Delivers [gI1, gI2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Generating secret key based on identity information and secret information (Fig 3 and 4, Tanaka).
- Generating at a first entity a first common key by using the secret key of the first entity and identity based public key from a point mapped on an algebraic curve of the second entity / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka), Fig. 8 shows the common key formula based on IB1 andIB2 (public key obtained by algebraic hashing function), and gA1 and gA2 (secret key).
- Generating a second common key ... / Similarly, B obtains Kab (Col 2, Line 13, Tanaka)
- Encrypting at the first entity a plaintext into a ciphertext by using the common key / Decrypting at the second entity a cipher text into a plaintext / Cryptosystem (Col 1, Line 21, Tanaka), Encrypting and decrypting data is central to a cryptosystem.

3. As to claims 2, 4, and 14:

- Generating/Obtaining a secret key by mapping at a point on an algebraic curve / Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Generating/Obtaining secret key based on identity information and secret information/ Calculates hashed identity information (Col 2, Line 8, Tanaka); Introduce two random numbers (secret information) (Col 1, Line 37 et seq., Tanaka); Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka);
- Generating/Obtaining a public key by using mapping at a point on the algebraic curve / A calculates B's hashed identity information using the one-way hash function (Col 2, Line 8, Tanaka)
- Generating/Obtaining at a first entity a first common key by using the secret key of the first entity and identity based public key / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka)

4. As to claim 12:

- Generating a secret key by mapping at a point on an algebraic curve / Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Generating secret key based on identity information and secret information/ Calculates hashed identity information (Col 2, Line 8, Tanaka); Introduce two

random numbers (secret information) (Col 1, Line 37 et seq., Tanaka); Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka);

5. As to claim 13:

- Generating a secret key by mapping at a point on an algebraic curve / Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Generating secret key based on identity information and secret information/ Calculates hashed identity information (Col 2, Line 8, Tanaka); Introduce two random numbers (secret information) (Col 1, Line 37 et seq., Tanaka); Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka);
- One way hash function to act on identity information and secret information / One way hash function (Col 1, Line 32, '755)

6. As to claim 15:

- Public key obtained by mapping at a point on the algebraic curve based on identity information of the second entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.
- Generating a common key by using the secret key of the first entity and identity based public key from a point mapped on an algebraic curve of the second entity / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka), Fig. 8 shows the common key formula based on IB1 andIB2

(public key obtained by algebraic hashing function), and gA1 and gA2 (secret key).

7. As to claim 16:

- A center generating a secret key of each entity by mapping at a point on an algebraic curve / Trusted center delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Generating secret key based on identity information and self-secret information / Calculates hashed identity information (Col 2, Line 8, Tanaka); Introduce two random numbers (secret information) (Col 1, Line 37 et seq., Tanaka); Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka)
- Generating a common key by using the self-secret key of the first entity and identity based public key from a point mapped on an algebraic curve of the second entity / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka), Fig. 8 shows the common key formula based on IB1 andIB2 (public key obtained by algebraic hashing function), and gA1 and gA2 (secret key).
- Common key used for encrypting/decrypting / Cryptosystem (Col 1, Line 21, Tanaka), Encrypting and decrypting data is central to a cryptosystem.

8. As to claim 17:

- Public key obtained by mapping at a point on the algebraic curve based on identity information of the entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.
- Generating a secret key by mapping at a point on an algebraic curve / Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Secret information / random numbers (Col 1, Line 37 et seq., Tanaka) used in calculation at a trusted center, (Col 2, Line 3, Tanaka)

9. As to claim 18:

- Causing the computer to input a secret key / Delivers [gl1, gl2] (secret key) through a secure channel (Col 2, Line 4, Tanaka)
- Public key obtained by mapping at a point on the algebraic curve based on identity information of a second entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.
- Generating a common key by using the secret key and the point mapped on an algebraic curve / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka), Fig. 8 shows the common key formula based on IB1 andIB2 (public key obtained by algebraic hashing function), and gA1 and gA2 (secret key).

10. As to claim 19:

- Public key obtained by mapping at a point on the algebraic curve based on identity information of a second entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.
- Generating a secret key by mapping at a point on an algebraic curve and secret information/ Delivers [gI1, gI2] (secret key) through a secure channel (Col 2, Line 4, Tanaka), a point mapped Algebraic curve is expressed in Figures 3 and 4.
- Secret information / random numbers (Col 1, Line 37 et seq., Tanaka) used in calculation at a trusted center, (Col 2, Line 3, Tanaka)

11. As to claim 20:

- Causing the computer to input a secret key / Delivers [gI1, gI2] (secret key) through a secure channel (Col 2, Line 4, Tanaka)
- Public key obtained by mapping at a point on the algebraic curve based on identity information of a second entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.
- Generating a common key by using the secret key and the point mapped on an algebraic curve / Party A performs the following simple calculation to share a common-key (Col 2, Line 11, Tanaka), Fig. 8 shows the common key formula based on IB1 andIB2 (public key obtained by algebraic hashing function), and gA1 and gA2 (secret key).

12. As to claim(s) 21:

Sharing is carried out between first and second entity utilizing magnitude relations between curves based on identity information of first and second entity / equation 8 utilizes magnitude relations for hashed identity information from first and second entities (Col 2, Paragraph 2, Fig 8, Tanaka)

13. As to claim(s) 22:

Key sharing is carried out between first and second entity by utilizing a symmetrical function / symmetric function (Fig 8, Tanaka)

14. As to claim(s) 23:

Secret key generated by multiplying a result of mapping at a point on an algebraic curve based on identity information by secret information (Figs 1 and 2, Tanaka)

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 3, 5, 6, and 8-11 rejected under 35 U.S.C. 103(a) as being unpatentable over Tanaka in view of Miyaji et al., US Patent No 5272755 (hereafter referred to as '755).

17. As to claims 3 and 9:

Tanaka teaches an identity-based non-interactive key sharing cryptosystem using a cryptographic one-way hashing algorithm in a process to determine a common key. Tanaka does not teach for the one-way hashing function to be implemented with algebraic elliptical curve cryptography techniques using Weil pairing. '755 teaches a one-way elliptical curve function based public key cryptosystem using Weil pairing. It would have been obvious to a person of ordinary skill in the art at the time of invention to use the one-way elliptical curve function based public key cryptosystem techniques of '755 for the one-hashing function used by Tanaka to generate the common key. One of ordinary skill in the art at the time of invention would have been motivated to use the one-way elliptical curve function based public key cryptosystem techniques of '755 for the one-hashing function used by Tanaka to generate the common key because using elliptic curve techniques can provide faster public key cryptography (Page 480, Paragraph 8, Schneier).

18. As to claim 5:

Algebraic curve in which a discrete logarithm problem defined thereon cannot be defined in polynomial time / This is inherent to the elliptical curve cryptosystem in Tanaka as modified above.

19. As to claim 6:

Inverse numeric values are generated in a process in respective entities when sharing the key / Common Key generation K=B^a=a^b (Fig 1, '755)

20. As to claim 8:

Claim 8 corresponds to claim 3 and further comprises:

Key sharing is carried out by utilizing a bilinear mapping property / all symbols in (Figs 1-4, Tanaka) are pre-declared constants except for IDL and GL1 resulting in a bilinear equation

21. As to claim 10:

Key sharing based on identity / Identity based key sharing (Abstract, Tanaka)

Pairing defined on an algebraic curve is used to share a key / Weil Paring (Col 13, Line 40, '755)

Utilizing a secret key generated by using mapping at a point on the algebraic curve based on:

- Identity information of the first entity / Fig 3 and 4 show secret key generation formulas based on ID information (Col 1, Line 36 et seq., Tanaka) for each user (Col 2, Line 4, Tanaka)
- Secret information / random numbers (Col 1, Line 37 et seq., Tanaka) used in calculation at a trusted center, (Col 2, Line 3, Tanaka)
- Public key obtained by mapping at a point on the algebraic curve based on identity information of the second entity / Hashed identity information (Col 2, Line 8, Tanaka), hashes are preformed with algebraic formulas.

- Key sharing is carried out by utilizing a bilinear mapping property / all symbols in (Figs 1-4, Tanaka) are pre-declared constants except for IDL and GL1 resulting in a bilinear equation

22. As to claim 11:

Common key generated by utilizing a relationship of inverse between numeric values / Common Key generation K=B^a=a^b (Fig 1, '755)

23. Claim 7 rejected under 35 U.S.C. 103(a) as being unpatentable over Tanaka in view of Bruce Schneier, "Applied Cryptography".

24. As to claim 7:

Tanaka teaches an identity-based non-interactive key sharing cryptosystem using ID information to calculate a public key. Tanaka does not explicitly teach the capability for using a plurality of public keys. Schneier teaches capabilities of identity based public key cryptography to include generating public keys based on name and one or more of other identifiers (Page 115, Line 6, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention that several of a person's many personal identifiers could be individually hashed to form several different public keys. One of ordinary skill in the art at the time of invention would have been motivated to allow several of a person's many personal identifiers to be individually hashed to form several different public keys because it is typical that a person has

several identifiers corresponding to possible means for contact and so it would be advantageous to permit secure identity based public key cryptography to protect each of these channels.

Conclusion

25. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

26. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

28. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100